KHIE
KENTUCKY HEALTH INFORMATION EXCHANGE

GOVERNOR'S OFFICE OF ELECTRONIC HEALTH INFORMATION

INFORMATION ON RECENT OFFICE OF CIVIL RIGHTS ACTIVITIES

Karen Chrisman
Staff Attorney

Kentucky
UNBRIDLED SPIRIT

KHIE
KENTUCKY HEALTH INFORMATION EXCHANGE

Presentation at the

NIST/OCR HIPAA Security Assurance Conference

Office of Civil Rights presentation of

HIPAA Security Rule Enforcement Activity

Occurred on

May 11, 2011

Governor's Office of Electronic Health Information

243 Security complaints opened and reviewed in 2010

- 128 were resolved by

70 required corrective action

18 investigated and required no action

40 closed without investigation

OCR ENFORCEMENT ACTIVITIES

September 2009 to April 2011

265 reports involving a breach of over 500 individuals

Theft and Loss are 67% of large breaches

Large breaches involving portable storage devices

- Laptop or desktop computers account for 53% of large breaches
- Paper records are 23% of large breaches

•31,000+ reports of breaches of under 500 individuals

OCR LESSONS LEARNED

OCR PRESENTED THE FOLLOWING AS LESSONS LEARNED:

- Do not neglect physical safeguards for areas where paper records are stored or used
- Reduce risk through network or enterprise storage as alternative to local devices
- Encryption of data at rest on any desktop or portable device/media storing EPHI is necessary
- Develop clear and well documented administrative and physical safeguards for storage devices and removable media which handle EPHI
- Raise the security awareness of workforce members and managers to promote good data stewardship

RECENT ENFORCEMENT ACTIONS

THE FOLLOWING SLIDES WERE PRESENTED AS EXAMPLES OF RECENT ENFORCEMENT ACTIONS BY THE OFFICE OF CIVIL RIGHTS

CIGNET HEALTH CARE

Cignet Health Care is a treatment provider and health plan issuer

- Over a two year period 41 individuals complained to OCR that Cignet ignored their requests for access to their health records
- Cignet failed to respond to OCR's investigation or provide copies of the patient's records

<u>PENALTY</u>

Civil Monetary Penalty of $1.3 million attributable to failure to provide individuals access to their health records

- Penalty of $3 million for failure to respond to OCR demands to produce records or cooperate in the investigation

TOTAL PENALTY 4.3 MILLION

MASSACHUSETTS GENERAL HOSPITAL

Large multi-specialty healthcare provider

Employee who had taken patient files home left the folders on the subway train and they were never recovered

Investigation initiated after media reports of incident and a complaint from an individual whose PHI was lost

Settled with OCR through Resolution Agreement and corrective action plan

NEEDED TO RESOLVE THE MATTER

$1 million resolution amount

Corrective Action Plan

MGH required to actively monitor its compliance with the Corrective Action Plan through an internal monitor

Revising, distributing policies & procedures regarding safeguards applied to PHI & EPHI away from the premises of the CE

Sanctioning workforce members who do not follow them

Training workforce members

Conducting internal monitoring

Submitting compliance reports to HHS for a period of three years

Management Services Organization of Washington

MSO provided practice management services to individual health care providers, an affiliated company, Washington Practice Management markets and sells Medicare Advantage plans to consumers for which it earns commissions

MSO disclosed EPHI to WPM without a valid authorization, so that WPM could market Medicare Advantage plans to those individuals. MSO had not developed or implemented appropriate and reasonable administrative, technical and physical safeguards to protect EPHI

- Actions required to settle with OCR
- $35,000 resolution about to OCR
- Corrective Action Plan
- ✓ Develop and implement policies and procedures to demonstrate compliance with the Privacy and Security Rules

  and that workforce training had occurred

Specifically the policies were required to be drafted to require
valid authorization for use or disclosure for marketing

the workforce had to be trained

the company had to prove the policies were made available to workforce and that workforce training occurred

- ✓ Submit compliance reports to HHS for a period of two years

Conclusions:

OCR aggressively enforcing the HIPAA Privacy and Security Rules

Covered entities and business associates should have robust HIPAA Privacy and Security compliance programs

A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents